FIG 1

[see drawing]

FIG 2

[see drawing]

Can be reached via API

FIG 3

[see drawing]

FIG 4

[see flow chart] [note: ja = yes; nein = no]

401   Logon

402   Start SWD   concurrent

          MONITORING

403   SWD secure?   Event or timer?

405   System secure?   Event treatment

406   Environment secure?

404   Defined termination, log

407   Start/run application

410   Wait for event

408   Application secure?

409   End?

          End

FIG 5

[see figure] [note: ja = yes; nein = no; Fkt = function]

Process X	APIHOOK.DLL	APIyy.DLL
APIFktCall ( )		
Error		
	APIFktHook ( )	
Normal return code		APIFkt ( ) stored code page
		APIFkt API code return
	IPC	
	Execute Fkt?	
SWD process		

FIG 6

[see figure] [note: ja = yes; nein = no; Fkt = function]

Secret
Virtual Memory Page

PAGE NO ACCESS

Change only via
API Fkt
VirtualProtect..( )

Process X
APIFktCall ( )

APIHOOK.DLL

PAGE EXECUTE
APIyy.DLL

APIFkt* ( )
API code start
secured in code page

Error!

APIHookFkt ( )
IS_CALLED = TRUE

Execute FKT?

External access
legal?

Normal
return code

Error!   jmp

Modified
API function
APIFktPatch ( ):
jmp
Continued API code

jmp HOOKAPIReturn

APIHookFktReturn ( )
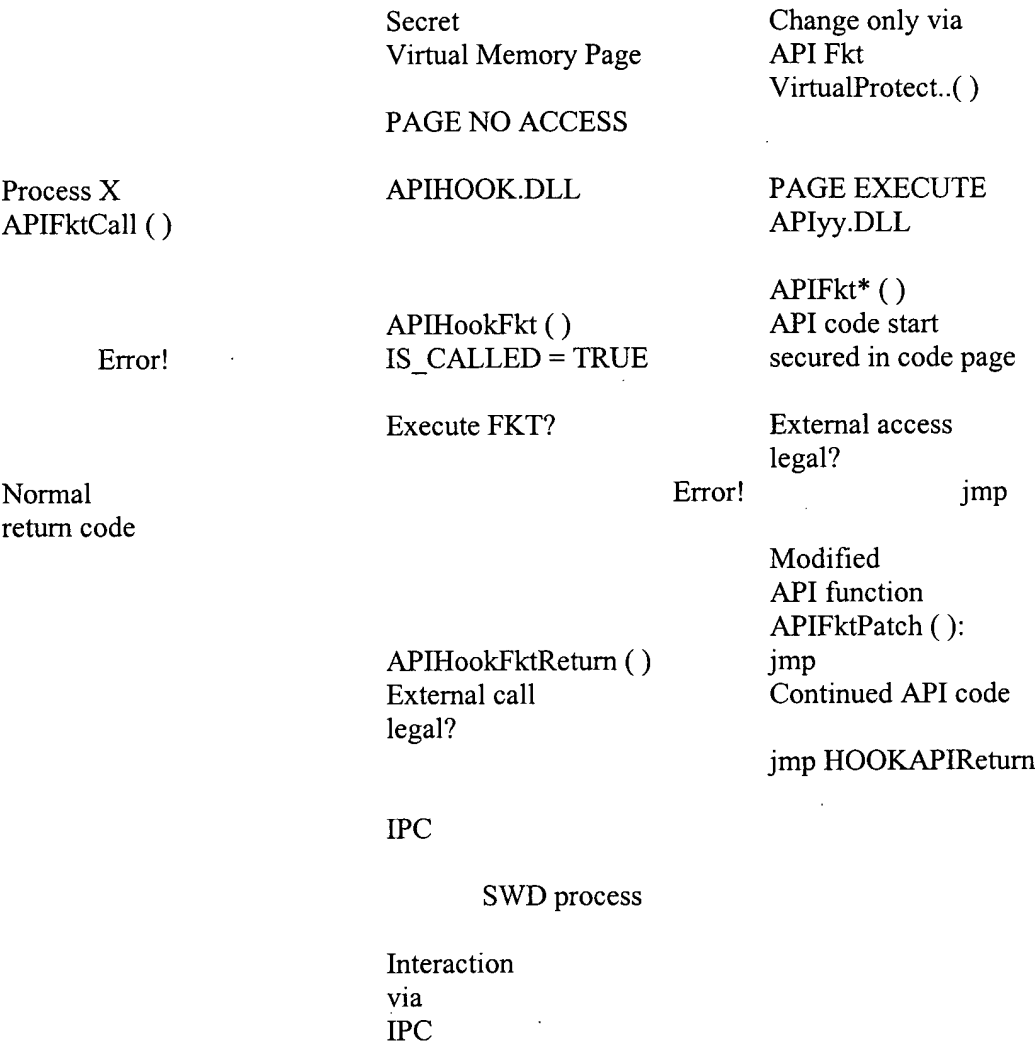External call
legal?

IPC

SWD process

Interaction
via
IPC

FIG 7

[see figure] [note: ja = yes; nein = no; Fkt = function]

Applications

API interception

Kernel32.DLL, GD132.DLL, User32.DLL

NTDLL.DLL

USER MODE

NTOSKRNL.EXE   WIN32K.EXE

Kernel interception

KERNEL MODE

HAL, driver